REMARKS

This communication is a response to the aforementioned non-final Office Action dated September 3, 2008. Claims 1-4, 11-14, 19 and 24-26, as presented in the Amendment filed on June 23, 2008, are not amended and remain in the application. Claims 1, 11 and 19 are independent.

Reconsideration of the application and withdrawal of the rejections of the claims are respectfully requested in view of the following remarks.

I. Rejections Under 35 U.S.C. § 103(a)

Claims 1-4, 11-14, 19 and 24-26 were rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Togawa et al. (U.S. Patent No. 5,918,008, hereinafter "Togawa") in view of Applicant's Admitted Prior Art (hereinafter "AAPA"). This rejection is respectfully traversed for the following reasons.

In the remarks of the June 23, 2008 Amendment, Applicant demonstrated how the claimed invention is markedly different from virus detection and prevention systems for use with general-purpose computers. However, in view of the new references applied by the Office in the present Office Action, it appears that the Office did not fully appreciate the fundamental distinctions between the claimed invention and such conventional systems.

Accordingly, before demonstrating that the applied references do not disclose or suggest all the recited features of the claimed invention, Applicant presents the following discussion of exemplary embodiments of the present invention to illustrate the fundamental differences between the claimed invention and conventional systems for use with general-purpose computers, such as the system of Togawa.

A. Exemplary Embodiments

Exemplary embodiments of the present invention provide a method and computer program for causing a controlling apparatus intended to control an image forming apparatus, as well as a controlling apparatus for controlling an image forming apparatus. One example configuration of the controlling apparatus is illustrated in Figure 1, in which a computer 200 is limited to controlling an image

forming apparatus such as copying machine 300 (see paragraph [0023] on page 7 of the specification).

As illustrated in Figure 3, a hard disk 204 of the computer 200 includes a database 240 in which a file list 241 is stored. The file list 241 is a list of all files, such as programs, required to exist in a specific storage area of a logical drive of hard disk 204 for controlling a multifunctional peripheral (MFP) 100 that includes the computer 200 and copying machine 300 (see, e.g., paragraph [0039]). As described in paragraph [0041] on page 11, the file list 241 is set up prior to factory shipment of MFP 100 and the controlling apparatus, and is stored in the hard disk 204 of the controlling apparatus. Accordingly, the file list 241 is a preset list of programs and files that are authorized to be run on the controlling apparatus to control the image forming apparatus, such as the copying machine 300 illustrated in Figure 1, for example.

According to the exemplary configuration in which the controlling apparatus (e.g., computer 200) is limited to controlling an image forming apparatus, the controlling apparatus is different from a general-purpose computing device in which a user may wish to add, modify or remove programs and files at will for various purposes. On the other hand, since the function of the controlling apparatus is limited to controlling the image forming apparatus, according to the exemplary configuration illustrated in Figure 1, the preset list of programs in the file list 241 represents a limited number of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus.

Therefore, the disclosed embodiments provide that programs that are authorized to be run to control the image forming apparatus are included in a preset list 241 of programs, and the preset list 241 is stored in the controlling apparatus (e.g., computer 200). This preset list 241 therefore contains programs that are known (approved) to control the image forming apparatus (e.g., copying machine 300). However, if a program is confirmed to be running on the controlling apparatus and that confirmed program is not included in the preset list of programs, the confirmed program is judged to be an illegal program resulting from a computer virus infection.

When a computer virus infiltrates into a computer, the virus often creates a new program and/or file. In the case of a general-purpose computing device, the number of programs and files that can be run is not limited to a preset list, because of the desire to allow users to add new programs or files and modify or delete existing programs or files. For example, general purpose computing devices are configured to allow users to add software programs containing executable and non-executable files, and add new non-executable files, such as a word processing document, for example. Therefore, conventional virus detection systems seek to compare a file against files that are known to be created by known viruses.

On the other hand, since the preset list of programs in the file list 241 represents a limited number of programs that are authorized be run on the controlling apparatus to control the image forming apparatus, the detection of a program that is not included in the file list 241 is judged to be an illegal program resulting from a computer virus infection. This judgment can be carried out because a limited number of programs that are authorized to be run on the controlling apparatus are stored in the preset list of programs.

These features of the disclosed embodiment are disadvantageous to the functions and purpose of a general-purpose computer. In particular, limiting a general-purpose computer to a preset list of programs would defeat the purpose of permitting a user to create, add and modify files and programs on the general-purpose computer. On the contrary, general-purpose computers are designed to allow dynamic modifications. Consequently, virus detection and prevention systems for general-purpose computers detect programs do not judge a file or program that is not included in a list of authorized programs or files to be an illegal program resulting from a computer virus, because such a system would severely limit the functionality of a general-purpose computer in allowing its user to create, add and/or modify existing files with the general-purpose computer.

B. Claimed Invention

Claims 1, 11 and 19 broadly encompass various features of the above-described exemplary embodiment.

Claim 1 recites a computer program stored on a computer-readable recording medium and causing a controlling apparatus intended to control an image forming apparatus to execute the following procedures:

(1) storing a preset list of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus;

(2) confirming each program running on the controlling apparatus;

(3) judging a program, which is **not included** in the preset list of programs that are authorized be run to control the image forming apparatus among programs whose running states have been confirmed, as an illegal program resulting from a computer virus infection; and

(4) deleting or isolating the program that is judged to be the illegal program.

Claim 11 recites a controlling apparatus for controlling an image forming apparatus. The controlling apparatus of claim 11 comprises a storage unit for storing in advance a preset list of programs that are authorized to be run for controlling the image forming apparatus. The controlling apparatus of claim 11 also comprises a processor that is configured to perform functions corresponding to procedures (2)-(3) of claim 1.

Claim 19 recites a controlling method for a controlling apparatus intended to control an image forming apparatus. The method of claim 19 comprises steps corresponding to procedures (1)-(4) of claim 1.

Accordingly, features (1)-(3) of claim 1 are common to each of independent claims 1, 11 and 19. Claims 1, 11 and 19 thus each recite that a preset list of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus are stored. In addition, claims 1, 11 and 19 each recite that each program running on the controlling apparatus is confirmed, and a program, which is **not included** in the preset list of programs that are authorized be run to control the image forming apparatus among programs whose running states have been confirmed, as an illegal program resulting from a computer virus infection.

Thus, claims 1, 11 and 19 recite that programs that are authorized to be run to control the image forming apparatus are included in a preset list of programs, and that the preset list of programs is stored. This preset list therefore contains programs that are known (approved) to control the image forming apparatus.

However, if a program is confirmed to be running on the controlling apparatus and that confirmed program is **not included** in the preset list of programs, the confirmed program is judged to be an illegal program resulting from a computer virus infection.

Togawa discloses a storage device for storing files and preventing the files stored thereon from being infected with a computer virus. The function of the storage device of Togawa is to have the ability to freely use files stored thereon with a personal computer while preventing the breeding of a virus and to delete a file infected with a virus or restore the infected file into an uninfected state (see Column 1, lines 25-28).

With reference to Figure 2, the storage device 1 includes a disk 10 on which files a stored, a first managing means 11, a second managing means 12, a file registering means 13, a virus checker 15, an infection management table means 16, a table registering means 17, and a judging means 18 (see Column 7, lines 39-47). The first managing means 11 manages original information of the stored on the disk 10, or manages original information of the virus checker 15. The second managing means 12 manages differential information concerning upgraded versions of the files stored on the disk 10 (i.e., version update information), and history information concerning the differential information brought about due to modification (i.e., version update history information). Alternatively, the second managing means 12 manages differential information concerning an upgraded version of the virus checker 15 (i.e., virus definition update information), and history information concerning the history of modifications of the information of the virus checker 15 (i.e., virus definition update history information) (see Column 7, lines 49-61).

The file registering means 13 reconciles the original information of the files stored on the disk 10 with the differential information (i.e., version update information) of the files stored on the disk 10, so that the file(s) can be reproduced. A generating means 14 performs a similar reconciliation operation between the original information of the virus definitions in the virus checker 15 and the virus definition update information of the virus checker 15 (see Column 8, lines 6-17).

The virus checker 15 can be activated at periodic intervals or on command (see Column 8, lines 18-21). The infection file management table means 16 is used to manage files stored on the disk 10 and to see if the stored files are infected with a

virus. The table registering means 17 registers data in the infection management table means 16. In particular, the table registering means 17 registers a virus-infected file detected by the virus checker 15 in the infection management table means 16 (see Column 8, lines 21-28 and 58). Accordingly, the infection file management table means 16 functions as a repository for virus-infected files, and the table registering means 17 writes the virus-infected files into the infection management table means 16.

When a request for access to one of the files stored on the disk 10 is received, the judging means 18 references the infection file management table means 16 to determine if the requested file is infected with a virus. That is, the judging means 18 references the infection file management table means 16 to determine if the requested file is registered in the infection file management table means 16, in which case it is judged that the requested file is infected with a virus (see Column 8, lines 25-29).

Figure 3 of Togawa illustrates an implementation of the storage device 1 being connected to a personal computer 2a, i.e., a general-purpose computer (see Column 10, lines 11-13). As illustrated in Figure 3, the storage device 1 includes an original information management file 34 that corresponds to the first managing means 11 of Figure 2. In particular, the original information management file 34 used to manage original information of files stored in the disk 30, and original information of a virus checker prepared for inspecting the files stored on the disk 30 (see Column 10, lines 23-27). The storage device 1 also includes a version upgrade information management file 35 that corresponds to the second managing means 12 of Figure 2. In particular, the version information management file 35 is used to manage differential information (i.e., version update information) concerning a file stored in the disk 30, and history information (i.e., version update history information) concerning the differential information brought about due to modification. In addition, the version information management file 35 is used to manage differential information concerning an upgraded version of the virus checker (i.e., virus definition update information), and history information concerning the history of modifications of the information of the virus checker (i.e., virus definition update history information) (see Column 10, lines 34-35).

In an attempt to arrive at the claimed invention, the Office asserted that the original information management file 34 corresponds to the preset list of programs as recited in claims 1, 11 and 19, and that the controller 38 (see Figures 3 and 5-9) corresponds to the controlling apparatus as recited in claims 1, 11 and 19.

These assertions are not supportable for the following reasons.

First, Togawa does not disclose or suggest that the original information management file 34 stores files to control the controller 38. On the contrary, Togawa merely discloses that the files identified in the original information management table 34 represent the files that are stored on the disk 30. The controller 38 accesses files stored on the disk 30, original information managed in the original information management file 34, and accesses the differential information (version update information of the files and virus definition version update information of the virus checker) in the version upgrade information management file 35 (see Column 10, line 66 to Column 11, line 5).

It is unclear how the Office reached its unsupported interpretation that the original information stored in the original information management file 34 somehow controls the controller 38. Furthermore, Togawa does not disclose or suggest that the original information stored in the original information management file 34 has been authorized to be run by the controller 38. The storage device 1 of Togawa is, as mentioned above, for use with a general-purpose computer (e.g., personal computer 2a). Therefore, it is antithetical and disadvantageous for the function of the personal computer 2a to have limited uses and functions by having a limited number of files and/or programs stored in the original information management file 34 for supposedly controlling the controller 38.

Furthermore, and most fundamentally, the Office's assertion that Togawa discloses the judging operation of claims 1, 11 and 19 is not supported by the disclosure of Togawa. In particular, the system of Togawa requires *a priori* knowledge of whether a file or program constitutes a virus, or else the virus checker would not be capable of detecting if a file stored on the disk 30 is infected with the virus. This is evidenced by the need for original information of the virus checker, as well as the differential information of the virus checker, which is virus definition version update information.

Togawa does not disclose, suggest or even contemplate that a file that is **not included** in the original information management file 34 is judged to be a file having been infected with a virus. On the contrary, Togawa discloses an entirely different configuration, in which the virus checker compares files that **are included** in the original information management file 34 with reference to the original information of the virus checker and any updated virus definition information (differential information) of the virus checker.

The Office appears to not fully appreciate the foundational distinction between the claimed invention and systems such as Togawa which are for use with general-purpose computers. Claims 1, 11 and 19 recite that a program which is **not included** in the preset list of programs is judged to be an illegal program resulting from a computer virus infection. On the other hand, Togawa discloses that files that **are included** in the original information management file 34 are checked for viruses.

The virus checker of Togawa determines whether files stored on the disk 30 are infected with a virus. The files stored on the disk 30 are identified in the original information management file 34. Therefore, any judgment of whether a file has been corrupted by a virus involves determining whether a file which **is included** in the original information management file 34 has been infected with a virus. On page 4 of the Office Action, the Office reasoned that because the original information stored in the original information management file 34 can be updated and stored as differential information, that the updating of the original information somehow corresponds to the judging operation of claims 1, 11 and 19. It is unclear how updating original information is related in any way to judging that a file which is **not included** in a preset list of authorized programs is an illegal file. On the contrary, the fact that the original information stored in the original information management file 34 can be updated contradicts the Office's unsupportable interpretation of Togawa. For the original information to be updated, it must therefore have already been stored. Information cannot be updated unless it has been stored previously. Therefore, the virus checking operation of Togawa and the subsequent quarantining of infected files involves a judgment of files **which are included** in the disk 30 and therefore **are included** in the original information management file 34.

Therefore, Applicant respectfully submits that Togawa does not disclose, suggest or contemplate that files which are **not included** in the original information management file 34 are judged to be illegal files resulting from a computer virus infection. On the contrary, Togawa discloses the opposite configuration.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that Togawa does not disclose or suggest:

(1) storing a preset list of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus; and

(3) judging a program, which is **not included** in a preset list of programs that are authorized be run to control the image forming apparatus among programs whose running states have been confirmed, as an illegal program resulting from a computer virus infection, as recited in claims 1, 11 and 19.

Furthermore, Applicant respectfully submits one skilled in the art would not have reason or been motivated to modify Togawa to arrive at the subject matter of claims 1, 11 and 19. The technique of Togawa is disclosed for general purpose computing devices, not for a controlling apparatus intended to control an image forming apparatus in which the programs that are authorized to be run therefor are included in a preset list of programs.

Similar to Togawa, AAPA also does not disclose or suggest storing a preset list of programs that are authorized to be run to control an image information apparatus, and judging a program which is **not included** in the preset list of programs as an illegal program resulting from a computer virus infection, as recited in claims 1, 11 and 19.

Consequently, AAPA does not cure the deficiencies of Togawa for failing to disclose or suggest all the recited features of claims 1, 11 and 19.

Therefore, no obvious combination of Togawa and AAPA can result in the subject matter of claims 1, 11 and 19, since Togawa and AAPA, either individually or in combination, fail to disclose or suggest all the recited features of claims 1, 11 and 19.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that claims 1, 11 and 19, as well as claims 2-4, 12-14 and 24-26 which depend therefrom, are patentable over Togawa and AAPA.

Dependent claims 2-4, 12-14 and 24-26 recite further distinguishing features over Togawa and AAPA, and are also patentable by virtue of depending from claims 1, 11 and 19.

The foregoing explanation of the patentability of claims 1, 11 and 19 is sufficiently clear such that it is believed to be unnecessary to separately demonstrate the patentability of the dependent claims at this time. However, Applicant reserves the right to do should it become appropriate. Furthermore, Applicant does not acquiesce to any of the Office's assertions not specifically addressed above. Applicant reserves the right to address any of the Office's assertions not specifically addressed above, should it become appropriate.

II. Conclusion

In view of the foregoing remarks, it is respectfully submitted that the present application is clearly in condition for allowance. Accordingly, a favorable examination and consideration of the instant application are respectfully requested.

If, after reviewing this response, the Examiner believes there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: December 29, 2008

By: /Jonathan R. Bowser/
Jonathan R. Bowser
Registration No. 54574

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620